AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.-56. (canceled)

57. (previously presented) A method of transferring authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the method comprising:

receiving a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

updating a first device history table to indicate that the first device is not authorized to render the protected electronic content and updating a second device history table to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

communicating a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device cryptographic key of the second device so that only the second device may gain access to the content cryptographic key by use of the device cryptographic key of the second device.

58. (previously presented) The method of claim 57 wherein the device cryptographic key of the second device is a symmetric key.

59. (previously presented) The method of claim 58 wherein the device cryptographic key of the second device is a DES key.

60. (previously presented) The method of claim 57 wherein the device cryptographic key of the second device is a public key having a corresponding private key stored with the second device, and protecting the content cryptographic key using the device cryptographic key of the second device includes protecting the content cryptographic key with the public key such that the second device may use the corresponding private key to gain access to the content cryptographic key.

61. (previously presented) The method of claim 60 wherein the public key is an RSA public key and the private key is an RSA private key.

62. (previously presented) The method of claim 57 wherein the content cryptographic key is a symmetric key which is used to encrypt the protected electronic content such that only the symmetric key can be used to decrypt the content.

63. (previously presented) The method of claim 57 further comprising receiving payment authorization information associated with the transfer authorization request, and charging a service fee based on the payment authorization information.

64. (previously presented) The method of claim 57 wherein updating the first device history table comprises removing a stored indicator of the protected electronic content from the first device history table.

65. (previously presented) The method of claim 57 wherein updating the first device history table comprises adding indicia that the protected electronic content is no longer authorized for the first device.

66. (previously presented) The method of claim 57 wherein the protected electronic content is audio content.

67. (previously presented) The method of claim 57 wherein the protected electronic content is video content.

68. (previously presented) The method of claim 57 wherein the protected electronic content is electronic written content.

69. (previously presented) The method of claim 57 wherein the indicator of the first device in the transfer authorization request is a unique serial number.

70. (previously presented) The method of claim 57 further comprising verifying that the first device is authorized to render the protected electronic content.

71.-82. (canceled)

83. (previously presented) A system of transferring authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the system comprising:

an input for receiving a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

a processor for updating a first device history table to indicate that the first device is not authorized to render the protected electronic content and updating a second device history table to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

an output for communicating a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device cryptographic key of the second device so that only the second device may gain access to the content cryptographic key by use of the device cryptographic key of the second device.

84. (previously presented) The system of claim 83 wherein the device cryptographic key of the second device is a symmetric key.

85. (previously presented) The system of claim 83 wherein the device cryptographic key of the second device is a public key having a corresponding private key stored with the second device, and protecting the content cryptographic key using the device cryptographic key of the second device includes protecting the content cryptographic key with the public key such that the second device may use the corresponding private key to gain access to the content cryptographic key.

86. (previously presented) The system of claim 83 wherein the content cryptographic key is a symmetric key which is used to encrypt the protected electronic content such that only the symmetric key can be used to decrypt the content.

87. (previously presented) The system of claim 83 wherein the input receives payment authorization information associated with the authorization request, and the processor charges a service fee based on the payment authorization information.

88. (previously presented) The system of claim 83 wherein the indicator of the first device in the transfer authorization request is a unique serial number.

89. (previously presented) The system of claim 83 wherein the processor verifies that the first device is authorized to render the protected electronic content.

90.-100. (canceled)

101. (currently amended) A method of transferring authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the method comprising:

receiving a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

updating a first device history table to indicate that the first device is not authorized to render the protected electronic content and updating a second device history

table to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

communicating a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device cryptographic key of the second device so that only the second device may gain access to the content cryptographic key by use of the device cryptographic key of the second device;

~~The method as in claim 57~~ wherein the first and second devices are devices which may be inserted into a standard tape player having a plurality of conventional user controls.

102. (canceled)

103. (currently amended) A system of transferring authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the system comprising:

an input for receiving a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

a processor for updating a first device history table to indicate that the first device is not authorized to render the protected electronic content and updating a second device history table to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

an output for communicating a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device cryptographic key of the second device so that only the second device may gain access to the content cryptographic key by use of the device cryptographic key of the second device;

~~The system as in claim 83~~ wherein the first and second devices are devices which may be inserted into a standard tape player having a plurality of conventional user controls.

104.-108. (canceled)

109. (previously presented) A method of operating a device manager to transfer authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the device manager being a different device than the first and second devices, the method comprising:

receiving, at the device manager, a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

updating a first device history table stored by the device manager to indicate that the first device is not authorized to render the protected electronic content and updating a second device history table stored by the device manager to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

communicating from the device manager a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device cryptographic key of the second device so that only the second device may gain access to the content cryptographic key by use of the device cryptographic key of the second device.

110. (previously presented) The method of claim 109 wherein the device cryptographic key of the second device is a symmetric key.

111. (previously presented) The method of claim 109 wherein the device cryptographic key of the second device is a DES key.

112. (previously presented) The method of claim 109 wherein the device cryptographic key of the second device is a public key having a corresponding private key stored with the second device, and protecting the content cryptographic key using the device cryptographic key of the second device includes protecting the content cryptographic key with the public key such that the second device may use the corresponding private key to gain access to the content cryptographic key.

113. (previously presented) The method of claim 112 wherein the public key is an RSA public key and the private key is an RSA private key.

114. (previously presented)The method of claim 109 wherein the content cryptographic key is a symmetric key which is used to encrypt the protected electronic content such that only the symmetric key can be used to decrypt the content.

115. (previously presented) The method of claim 109 further comprising receiving, at the device manager, payment authorization information associated with the transfer authorization request, and charging a service fee based on the payment authorization information.

116. (previously presented) The method of claim 109 wherein updating the first device history table comprises removing a stored indicator of the protected electronic content from the first device history table.

117. (previously presented) The method of claim 109 wherein updating the first device history table comprises adding indicia that the protected electronic content is no longer authorized for the first device.

118. (previously presented) The method of claim 109 wherein the protected electronic content is audio content.

119. (previously presented) The method of claim 109 wherein the protected electronic content is video content.

120. (previously presented) The method of claim 109 wherein the protected electronic content is electronic written content.

121. (previously presented) The method of claim 109 wherein the indicator of the first device in the transfer authorization request is a unique serial number.

122. (previously presented) The method of claim 109 further comprising verifying that the first device is authorized to render the protected electronic content.

123. (currently amended) A method of operating a device manager to transfer authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the device manager being a different device than the first and second devices, the method comprising:

receiving, at the device manager, a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

updating a first device history table stored by the device manager to indicate that the first device is not authorized to render the protected electronic content and updating a second device history table stored by the device manager to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

communicating from the device manager a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device

cryptographic key of the second device so that only the second device may gain access to the content cryptographic key by use of the device cryptographic key of the second device;

~~The method as in claim 109~~ wherein the first and second devices are devices which may be inserted into a standard tape player having a plurality of conventional user controls.

124. (previously presented) A device manager which is capable of transferring authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the device manager being a different device than the first and second devices, the device manager comprising:

a device manager input for receiving a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

a device manager processor for updating a first device history table to indicate that the first device is not authorized to render the protected electronic content and updating a second device history table to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

a device manager output for communicating a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device cryptographic key of the second device so that only the second device may gain

access to the content cryptographic key by use of the device cryptographic key of the second device.

125. (previously presented) The device manager of claim 124 wherein the device cryptographic key of the second device is a symmetric key.

126. (previously presented) The device manager of claim 124 wherein the device cryptographic key of the second device is a public key having a corresponding private key stored with the second device, and protecting the content cryptographic key using the device cryptographic key of the second device includes protecting the content cryptographic key with the public key such that the second device may use the corresponding private key to gain access to the content cryptographic key.

127. (previously presented) The device manager of claim 124 wherein the content cryptographic key is a symmetric key which is used to encrypt the protected electronic content such that only the symmetric key can be used to decrypt the content.

128. (previously presented) The device manager of claim 124 wherein the device manager input receives payment authorization information associated with the authorization request, and the processor charges a service fee based on the payment authorization information.

129. (previously presented) The device manager of claim 124 wherein the indicator of the first device in the transfer authorization request is a unique serial number.

130. (previously presented) The device manager of claim 124 wherein the device manager processor verifies that the first device is authorized to render the protected electronic content.

131. (currently amended) A device manager which is capable of transferring authorization to render protected electronic content from a first device to a second device having a device cryptographic key, the device manager being a different device than the first and second devices, the device manager comprising:

a device manager input for receiving a transfer authorization request having an indicator of the first device, an indicator of the second device, and an indicator of the protected electronic content;

a device manager processor for updating a first device history table to indicate that the first device is not authorized to render the protected electronic content and updating a second device history table to indicate that second device is authorized to render the protected electronic content based on the received transfer authorization request; and

a device manager output for communicating a transfer authorization response having an indicator of the second device, an indicator of the protected electronic content, and a content cryptographic key for the protected electronic content protected using the device cryptographic key of the second device so that only the second device may gain access to the content cryptographic key by use of the device cryptographic key of the second device;

~~The device manager as in claim 124~~ wherein the first and second devices are devices which may be inserted into a standard tape player having a plurality of conventional user controls.